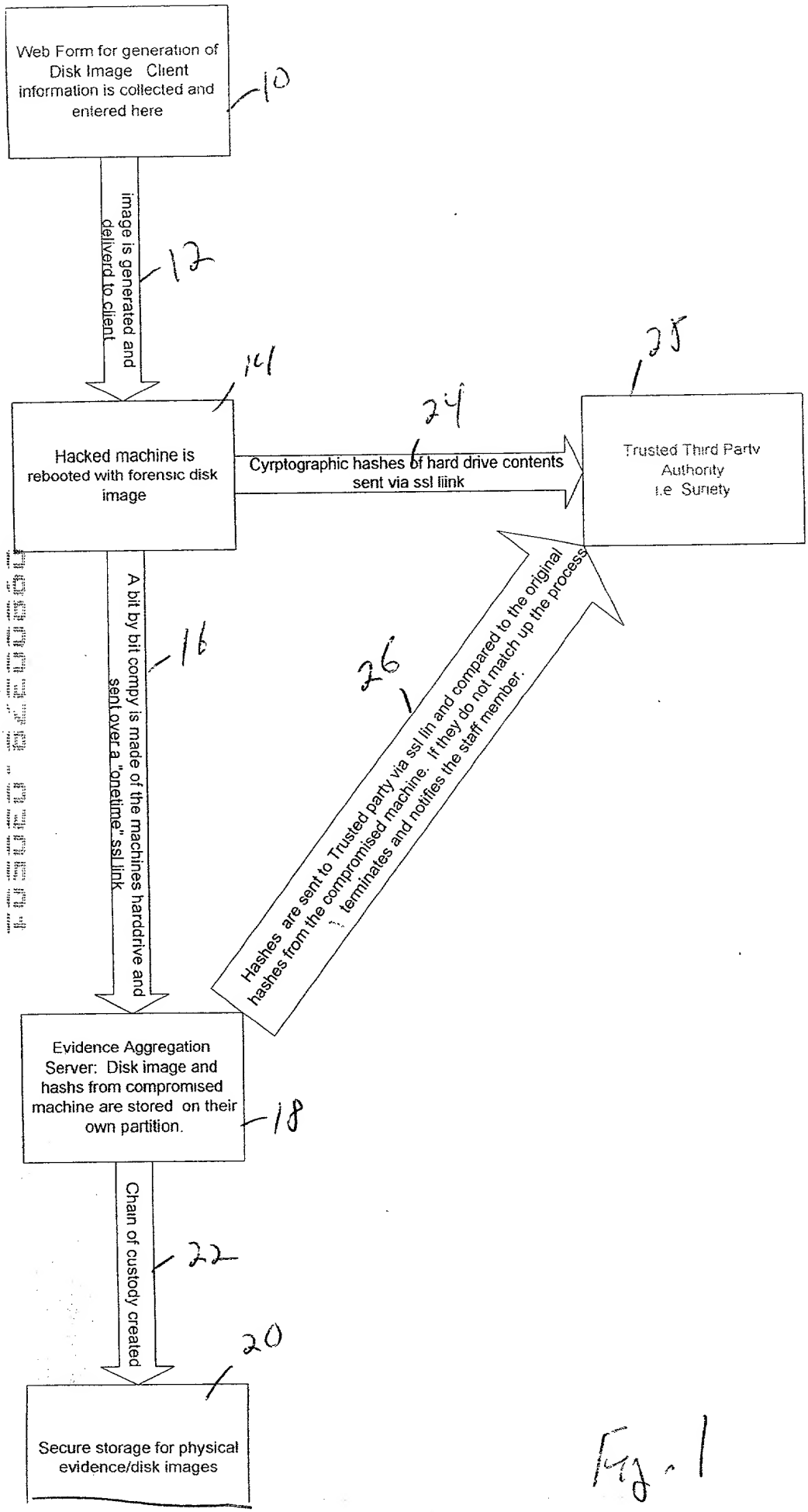
Web Form for generation of Disk Image Client information is collected and entered here
10
image is generated and deliverd to client
12
Hacked machine is rebooted with forensic disk image
14
Cyrptographic hashes of hard drive contents sent via ssl liink
24
Trusted Third Party Authority i.e Surety
25
A bit by bit compy is made of the machines harddrive and sent over a "onetime" ssl link
16
Hashes are sent to Trusted party via ssl lin and compared to the original hashes from the compromised machine. If they do not match up the process terminates and notifies the staff member.
26
Evidence Aggregation Server: Disk image and hashs from compromised machine are stored on their own partition.
18
Chain of custody created
22
Secure storage for physical evidence/disk images
20

Fig. 1